

Process Based Mission Assurance SecureMeeting User's Guide

**Prepared for the
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Report No. 0190602.17.001
Revision 2.1**

February 10, 2006

ARES CORPORATION

21000 Brook Park Road
MS OAI
Cleveland, OH 44135

TABLE OF CONTENTS

1.	INTRODUCTION.....	4
2.	SECURITY PRACTICES.....	5
2.1	ADMINISTRATIVELY CONTROLLED INFORMATION	5
2.2	PROTECTING LOGIN INFORMATION	5
2.3	MEETING MONITORING.....	5
2.3.1	<i>Meeting Security.....</i>	5
2.3.2	<i>Information.....</i>	6
3	PROCESS FOR OBTAINING A PBMA SECUREMEETING ACCOUNT.....	7
4	CREATING, ATTENDING, AND RUNNING MEETINGS	10
4.1	CREATING MEETINGS.....	10
4.1.1	<i>Creating Meetings through the New Meeting... Option</i>	<i>10</i>
4.1.2	<i>Creating Meetings through the Instant Meeting Option.....</i>	<i>11</i>
4.1.3	<i>Creating Meetings through the Microsoft Outlook Plug-in.....</i>	<i>14</i>
4.1.3.1	<i>Installing the SecureMeeting Plug-in for Microsoft Outlook</i>	<i>14</i>
4.1.3.2	<i>Scheduling Meetings Through Microsoft Outlook.....</i>	<i>15</i>
4.2	ATTENDING MEETINGS	18
4.2.1	<i>PBMA SecureMeeting Supported Environments</i>	<i>18</i>
4.2.1.1	<i>Operating system and browser requirements</i>	<i>18</i>
4.2.1.2	<i>Additional requirements and restrictions.....</i>	<i>19</i>
4.2.2	<i>Accessing the Meeting URL.....</i>	<i>19</i>
4.2.3	<i>Joining the Meeting</i>	<i>21</i>
4.2.4	<i>Meeting Viewer.....</i>	<i>22</i>
4.2.4	<i>Viewing a Meeting</i>	<i>22</i>
4.3	RUNNING MEETINGS	23
4.3.1	<i>Meeting Roles and Functionality.....</i>	<i>23</i>
4.3.2	<i>Passing Presenter Rights to Another Attendee</i>	<i>24</i>
4.3.3	<i>Passing Conductor Rights to Another Attendee.....</i>	<i>24</i>
4.3.4	<i>Passing Controller Rights to Another Attendee.....</i>	<i>24</i>
4.3.5	<i>Desktop Sharing</i>	<i>25</i>
4.3.6	<i>Secure Chat Functionality.....</i>	<i>27</i>
4.3.7	<i>Desktop Drawing.....</i>	<i>28</i>
4.3.8	<i>Removing Attendees.....</i>	<i>29</i>
4.3.9	<i>Extending Meetings</i>	<i>30</i>
4.3.10	<i>Closing Meetings</i>	<i>30</i>
5	GETTING HELP	31

TABLE OF FIGURES

Figure 1 - Process for Attaining a PBMA SecureMeeting Account.....	7
Figure 2 - Login to SecureMeeting Account Web Page	8
Figure 3 - The Preferences Link	8
Figure 4 - The Preferences Web Page.....	9
Figure 5 - The Meetings Page	10
Figure 6 - The Join Meeting Web Page	11
Figure 7 – Security Warning for Juniper Network’s Signed Applet	12
Figure 8 - Meeting Details Page (Part 1)	12
Figure 9 - Meeting Details Page (Part 2)	13
Figure 10 - Add Invitee Window	14
Figure 11 - MS Outlook Plug-in Setup	15
Figure 12 - Microsoft Outlook.....	16
Figure 13 - Outlook Appointment and Scheduling Interface.....	17
Figure 14 - The Check Meeting Compatibility Link	18
Figure 15 - Sample Invitation Email.....	20
Figure 16 - SecureMeeting Calendar	21
Figure 17 - The Join Meeting Button.....	21
Figure 18 - The Meeting Viewer Window.....	22
Figure 19 - The Share Application Window	26
Figure 20 - The Secure Meeting Chat Window	28
Figure 21 - A Drawing Sample showing Circles, Straight Lines, and Text	29
Figure 22 - The Help Link	31
Figure 23 - The Help Window	31

1. Introduction

Process Based Mission Assurance (PBMA) SecureMeeting is a collaboration tool that allows users to securely schedule and hold online meetings that involve Administratively Controlled Information (ACI) data. In meetings, users can share their complete desktops or individual applications over a 128-bit encrypted, secure connection. SecureMeeting attendees can also remote-control one another's desktops and chat using a separate application window that does not interfere with the presentation.

The only function of this system is to permit users to collaborate and display sensitive data through secure meeting functionality. This is a “virtual sharing” of visual information, which means no files are transmitted. Therefore, the system is nothing more than a pass-through for information to be shared via secure online meetings and does not retain any of the meeting data. This system is designed specifically for the sharing of ACI data through display only. This system is **not** certified nor accredited to handle or display classified national security information. Any sharing beyond specifically authorized individuals with a determined “need-to-know” is in violation of NASA Policy and may be in violation of Federal law.

Proper safeguarding is the responsibility of the individual in possession of ACI material to protect it from access by, or disclosure to, unauthorized persons. This means that it is incumbent upon each SecureMeeting account holder to protect the meetings in which they are conducting or attending.

For all open, non-ACI discussions please make use of NASA's WebEx tool.

SecureMeeting is targeted to customers in need of highly secure Web casting services employing 128-bit encryption from the NASA firewall. WebEx is NASA's standard web casting application and should be used for all normal web casting activities. SecureMeeting is not an alternative to WebEx, it is an add-on service for secure communication.

2. Security Practices

All individuals who partake in secure meetings must take responsibility for protecting Administratively Controlled Information (ACI). ACI information must be safeguarded by protecting login information and restricting meeting access to only those who possess a need-to-know for the sensitive information being presented.

2.1 *Administratively Controlled Information*

Administratively Controlled Information is official information and material, of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified), nonetheless, should still be protected against inappropriate disclosure. Within NASA, such information may have previously been designated “FOR OFFICIAL USE ONLY.” This NASA designation has been changed to “Administratively Controlled Information,” for clarity and to more accurately describe the status of information to be protected.

2.2 *Protecting Login Information*

PBMA SecureMeeting accounts are granted only to individuals that have a need for meeting capability and are working on official NASA business. Access to the meeting application is governed by a login page that requires a user to enter a user name and password. Each individual shall have their own account and no accounts are to be shared without approval from NASA’s IT Security. Also, login information should never be recorded in an unprotected location - electronic or physical, where unauthorized individuals can access it.

2.3 *Meeting Monitoring*

2.3.1 Meeting Security

Individuals with PBMA SecureMeeting accounts are responsible for ensuring that meeting attendance is limited to individuals with a legitimate need-to-know for the sensitive information being shared. Good security practices include:

- Always attending the system when in use.
- Ensuring that the system is inaccessible by unauthorized individuals, if it is necessary to step away from the system for any reason during the meeting.
- Verifying that all attendees are eligible to have access to the information being presented in the meeting. If the meeting scheduler is not the Data Owner, check with the Data Owner to make sure that appropriate checks on meeting invitees have been conducted so that no unauthorized disclosures of the sensitive data occurs.
- Canceling meetings and notifying meeting invitees of cancellations.
- Removing meeting attendees as data is presented for which they do not have a need-to-know.
- Requesting SecureMeeting account deactivation when no longer needed.

2.3.2 Information

Meeting schedulers should have complete and thorough knowledge of all material that is shared and displayed at their meetings. **It is imperative that sensitive data be protected at all times.** Criteria of at least one of the following must be met to qualify as ACI, as outlined in NPR 1600.1, *NASA Security Program Procedural Requirements*, Chapter 5.22:

- Information Protected by Statute: Export Administration Act; Arms Export Control Act; Space Act (Section 303b):
 - ♦ ITAR: International Traffic in Arms Regulations
 - ♦ EAR: Export Administration Regulations
 - ♦ MCTL: Military Critical Technologies List
 - ♦ FAR: Federal Acquisition Regulations
 - ♦ FOIA: Freedom of Information Act and the Privacy Act of 1996
 - ♦ UCNI: Unclassified Controlled Nuclear Information.
- Information the data owner determines to be unusually sensitive or critical to the success of the program or project
- Information Exempt from Freedom of Information Act (FOIA); which includes:
 - ♦ Internal Personnel Rules/Practices
 - ♦ Trade Secrets/Commercial/Financial
 - ♦ Inter/Intra-Agency Memos and Letters
 - ♦ Personnel and Medical Files
 - ♦ Investigative Records
 - ♦ Financial Institution Information
 - ♦ Geological/Geophysical
 - ♦ Maps/Documents of underground utilities
 - ♦ Drawings/specifications for Mission Essential Infrastructure (MEI) or other assets
 - ♦ Mission specific security plans
 - ♦ Emergency Contingency plans

3 Process for Obtaining a PBMA SecureMeeting Account

In order to setup and schedule meetings you must have a SecureMeeting account. **You must have a SecureMeeting account to attend meetings.** Figure 1 below outlines the process for obtaining a SecureMeeting account:

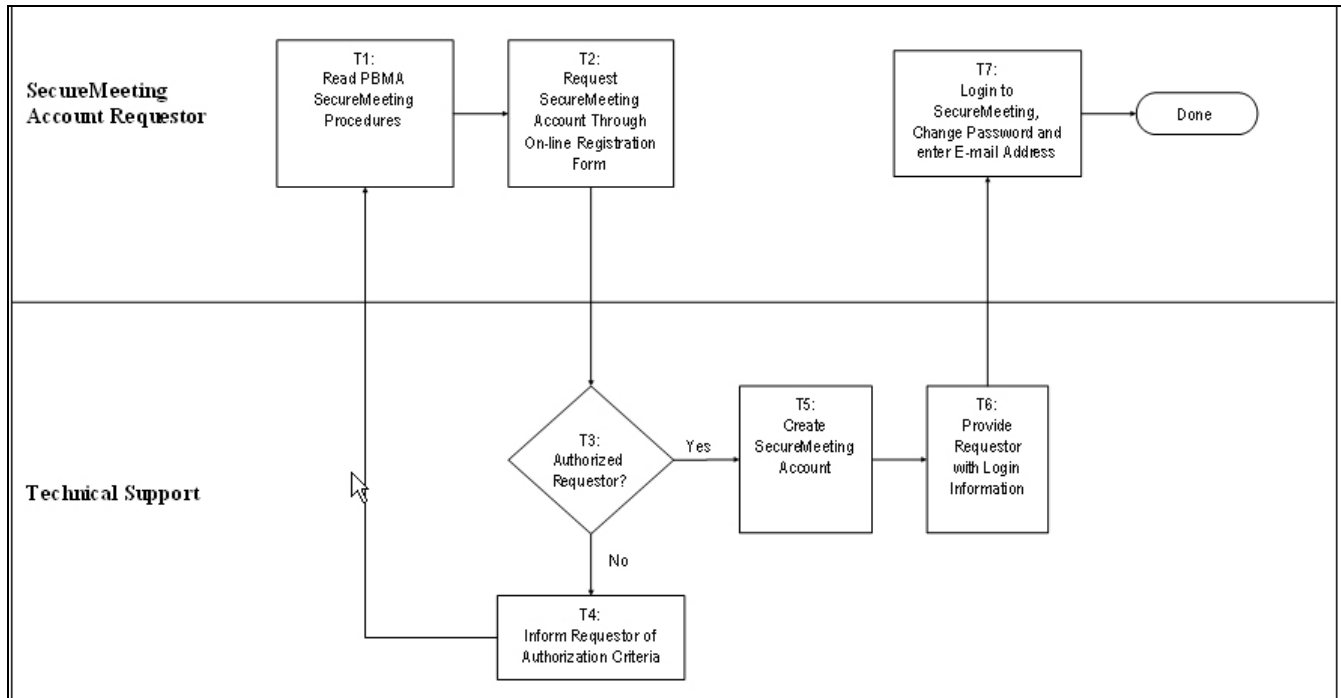


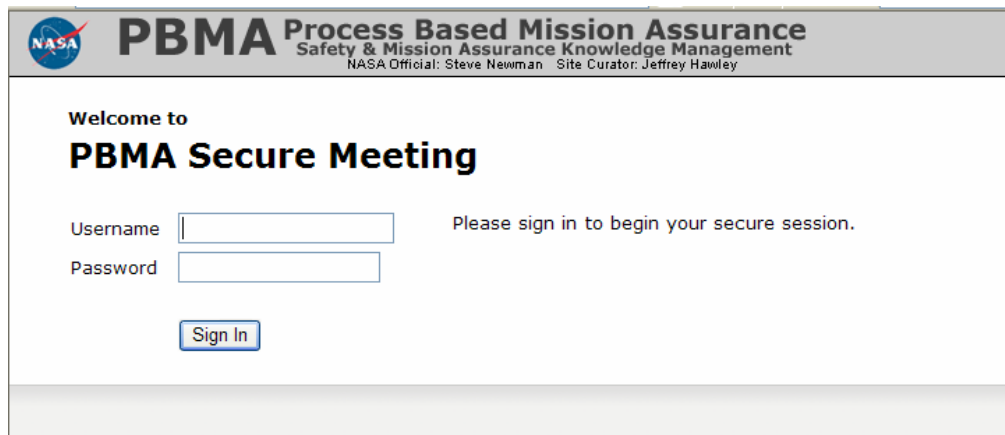
Figure 1 - Process for Attaining a PBMA SecureMeeting Account

- T1. *Read the PBMA SecureMeeting Procedures:* Any individual requesting a SecureMeeting account must read the *PBMA SecureMeeting Procedures* to become familiar with the purpose of the application and the responsibilities associated with it.
- T2. *Request SecureMeeting Account Through On-line Registration Form:* Request a SecureMeeting account through the PBMA-KMS Web site on-line registration form (http://pbma.nasa.gov/securemeeting_accountrequest).
- T3. *Authorized Requestor:* Determine if the Requestor is authorized to request a SecureMeeting account.
- T4. *Inform Requestor of Authorization Criteria:* If the requestor is not authorized to have a SecureMeeting account, refer them to the *PBMA SecureMeeting Procedures* for an explanation of authorization criteria.
- T5. *Create SecureMeeting Account:* Technical Support will create the requestor's SecureMeeting account
- T6. *Provide Requestor with Login Information:* Technical Support then provides the requestor with their user name and initial password by telephone.

- T7. *Login to SecureMeeting, Change Password and enter Email Address:*
Requestor logs into the site and changes their password.

Each user must change their password through the following steps:

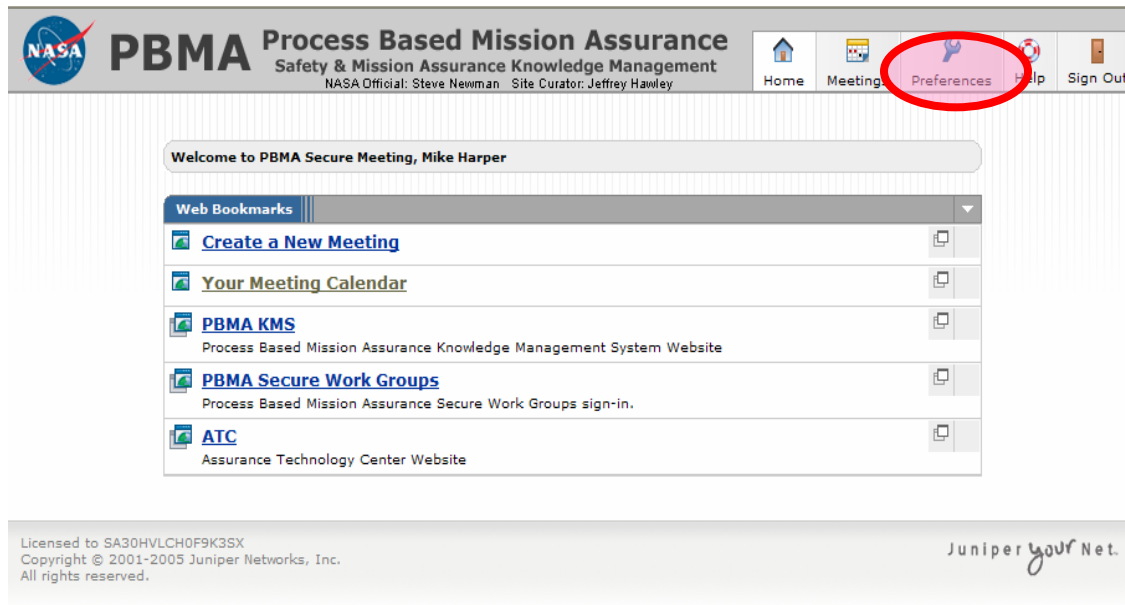
1. Log in through the **SecureMeeting Login** Web page located at <https://securemeeting.grc.nasa.gov>, shown in Figure 2 below.



The screenshot shows the login page for PBMA Secure Meeting. At the top, there is a NASA logo and the text "PBMA Process Based Mission Assurance Safety & Mission Assurance Knowledge Management NASA Official: Steve Newman Site Curator: Jeffrey Hawley". Below this, it says "Welcome to PBMA Secure Meeting". There are two input fields: "Username" and "Password". To the right of the "Username" field, it says "Please sign in to begin your secure session." Below the input fields is a "Sign In" button.

Figure 2 - Login to SecureMeeting Account Web Page

2. Click the *Preferences* link shown in Figure 3 below.



The screenshot shows the user interface after logging in. At the top, there is a NASA logo and the text "PBMA Process Based Mission Assurance Safety & Mission Assurance Knowledge Management NASA Official: Steve Newman Site Curator: Jeffrey Hawley". Below this, it says "Welcome to PBMA Secure Meeting, Mike Harper". There is a navigation bar with links: "Home", "Meeting", "Preferences", "Help", and "Sign Out". The "Preferences" link is highlighted with a red circle. Below the navigation bar, there is a "Web Bookmarks" section with links to "Create a New Meeting", "Your Meeting Calendar", "PBMA KMS", "PBMA Secure Work Groups", and "ATC". At the bottom, there is a footer with text: "Licensed to SA30HVLCH0F9K3SX Copyright © 2001-2005 Juniper Networks, Inc. All rights reserved." and the Juniper logo.

Figure 3 - The Preferences Link

3. You will be taken to the **Preferences** Web Page shown in Figure 4. Change

your password from the one that was given to you by PBMA Technical Support by typing in the appropriate fields.

4. Type your email address in the *Default Email Address* field.
5. Click the *Save* button to save your changes.

Note: If you have a dedicated teleconference number, you can enter that information in the *Default Teleconference Info* field and click the *Save* button next to it to save your changes.

PBMA Process Based Mission Assurance
Safety & Mission Assurance Knowledge Management
NASA Official: Steve Newman Site Curator: Jeffrey Hawley

Home Meetings Preferences Help Sign Out

Preferences

User Home General Applications Advanced

Change Name

Full Name:

Change Password

Old Password:
New Password:
Confirm Password:

Daylight Savings Time

Observe DST in this timezone:

Secure Meetings

Indicate where you would like to receive Secure Meeting email invitations. Invitations to the meetings that you schedule are sent from this account as well.

Default email address:

Default Teleconference Info: ☐ Enable

Licensed to SA30HVLCH0F9K3SX
Copyright © 2001-2005 Juniper Networks, Inc.
All rights reserved.

Juniper your Net.

Figure 4 - The Preferences Web Page

4 Creating, Attending, and Running Meetings

4.1 Creating Meetings

SecureMeeting users can create meetings in one of three ways:

1. through the *New Meeting...* button
2. through the *Instant Meeting* button
3. through the plug-in for Microsoft Outlook for those users who use the Microsoft Outlook client

4.1.1 Creating Meetings through the *New Meeting...* Option

To create a meeting through the “New Meeting...” button, the user must perform the following steps:

1. Once logged in, the user must click on the *Meeting* tab in the upper right-hand corner menu.
2. Click the *New Meeting...* button shown in Figure 5.

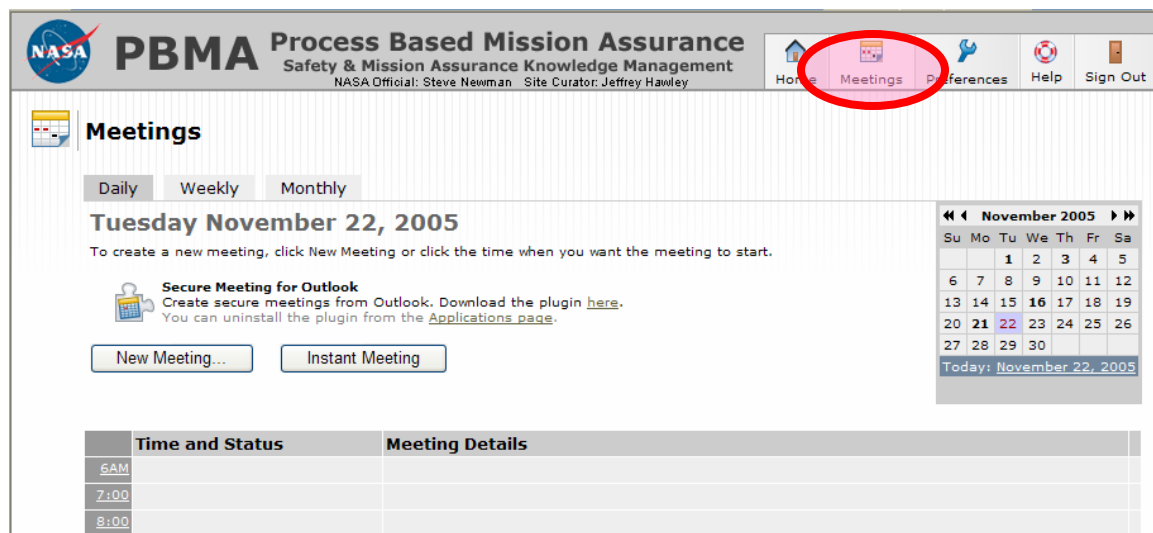


Figure 5 - The Meetings Page

3. Enter information in the following sections of the *Meeting Details* page if you do not want to use the default settings generated by the system:
 - [General Information Section](#)
 - [Date and Time Section](#)
 - [Invitees Section](#) - When the meeting creator specifies who they want to invite, the prospective attendee must have a SecureMeeting account. Therefore, if you add an email of an individual that does not have an account in the *Add Other Users* section of the *Details* page, they will receive the message but will not be able to join the meeting.

4. Once all meeting information sections are filled and invitees are added, select the “Save Changes” button.
5. Each invitee will receive an email that contains the meeting time, duration, date, agenda, teleconference information, meeting venue URL, and system compatibility checker URL.

4.1.2 Creating Meetings through the *Instant Meeting* Option

The meeting creator may choose to bypass most meeting scheduling steps and create an Instant Meeting. To create a meeting through the “Instant Meeting” button, the following steps must be performed:

1. Once logged in, the user must click on the *Meeting* tab in the upper right-hand corner menu.
2. Click the *Instant Meeting* button shown in Figure 5. The system automatically generates a meeting with a unique name to start immediately for a specified duration of 60 minutes, and adds the meeting creator as the only invitee.
3. This will generate the *Join Meeting* page on the meeting creator’s desktop as seen in Figure 6.

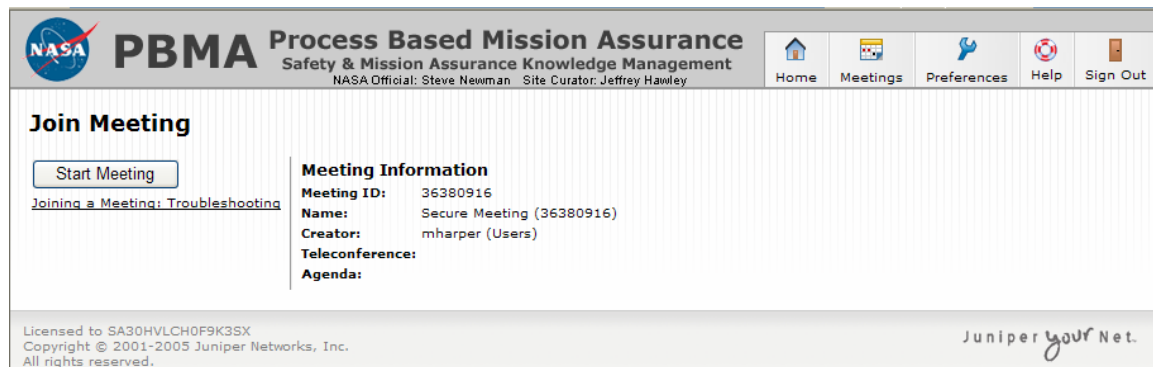


Figure 6 - The Join Meeting Web Page

4. Then, the meeting creator simply needs to click **Start Meeting** to begin.
5. When a meeting is launched, the security warning from Juniper Networks will appear as seen in Figure 7. This signed applet is safe and the user must choose “Yes” to launch the meeting on their desktop.

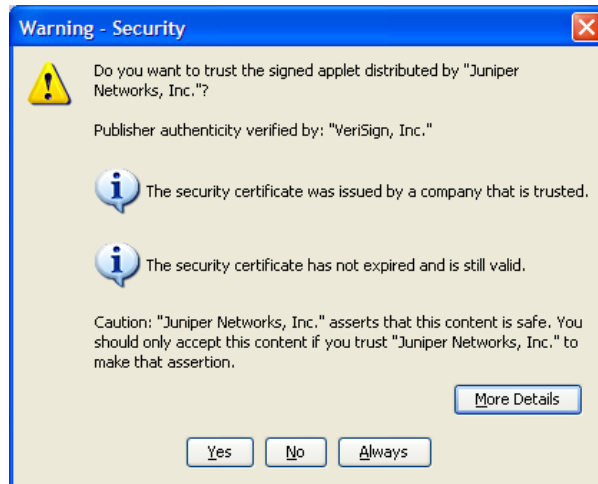


Figure 7 – Security Warning for Juniper Network’s Signed Applet

6. Once the *Details* link has been clicked, the **Meeting Details** Web page will appear as in Figure 8. Enter in the meeting’s name, teleconference info, and some quick details about the meeting’s agenda in the open text fields under the General Information section.

Meeting Details

Update

General Information

Meeting ID: 58038092

Unique ID for the meeting.

Created By: Michael Bellomo (Users)

Name:

Short topic for the meeting. If you leave the field blank, Secure Meeting randomly generates a name for you.

Teleconference Info:

Phone number invitees should call to join the meeting

Agenda:

Description of the meeting's purpose

Date and Time

Date: / /

Starting date, time, and duration for the meeting. To start the meeting immediately, use the default settings.

Start: :

Note: the time zone for the meeting is (GMT-08:00) Pacific Time (US & Canada); Tijuana

Duration: hours minutes

Recurring:

If you want to schedule more than one instance of the meeting, select a recurrence schedule.

Figure 8 - Meeting Details Page (Part 1)

Figure 9 - Meeting Details Page (Part 2)

7. This will return you to the **Meeting Details** Web page. Scroll to the bottom of the page to the **Save Changes** section as shown previously in **Error! Reference source not found..**
8. Select the available check box and then click the *Update* button to send out the meeting invitations. This will return you to the **Meeting** Web page where the Meeting Creator wait for the invitees to arrive and then run the meeting.
9. The SecureMeeting application will send an individual notification email to each invitee. **Again note that the “Add Other Users” feature (as shown previously in Error! Reference source not found.) that allows you to invite by email address works, but if the invitee does not have a SecureMetting account, they will not be able to join the meeting.**
4. The **Add Invitee** window will appear as in **Error! Reference source not found..** Type the username of the individual you wish to search for, in the open *Search for:* field or utilize the asterisk as a wildcard symbol as the window instructs to find your invitees.
5. Click the *Search for Users* button to commence the search. The results will appear immediately below.
6. Check the box next to the username of the individual(s) you want to invite and click the *Add Selected* button to populate the meeting.

Add Invitee

Local

Secure Meeting displays all users whose usernames contain the letters you enter below. For example, if you enter "ann", Secure Meeting displays users named "Ann", "Anne", and "Annika". You may also use a wildcard (*) within a string for the same purpose.

Search for:

Authentication Server:

1 matches found..

Username	Full Name:	Authentication Server
<input type="checkbox"/> mharper	Mike Harper	Administrators

[Check All](#) [Clear All](#)

Figure 10 - Add Invitee Window

7. This will return you to the **Meeting Details** (Figure 9) page. Scroll to the bottom of the page to the **Save Changes**.
8. Select the available check box and then click the *Finish* button to send out the meeting invitations. This will return you to the **Meeting Web** page where you wait for the invitees to arrive and then run the meeting.

When the meeting creator specifies who they want to invite, the prospective attendee must have a SecureMeeting account. The SecureMeeting application will send an individual notification email to each invitee.

4.1.3 Creating Meetings through the *Microsoft Outlook Plug-in*

The third option to schedule a SecureMeeting is through Microsoft Outlook. First, however, the meeting creator must use Microsoft Outlook as their mail client. Juniper provides the SecureMeeting plug-in for Outlook that must be installed as outlined in the following steps:

4.1.3.1 Installing the SecureMeeting Plug-in for Microsoft Outlook

- Close Microsoft Outlook.
- On the Meetings Page (Figure 5), under **Secure Meeting for Outlook**, click the link for downloading the plugin.
- Click **Yes** if a security warning (Figure 7) dialog box appears.
- Click **Install**.
- When Secure Meeting completes the installation, click **Finish**.
- When the **Secure Meeting Outlook Plugin Setup** dialog box appears, as seen in Figure 11, click **Provide Server Details** to specify details about

your login information when creating a meeting. By entering server information during installation, you create defaults that the plug-in may use for all meetings that you schedule. Otherwise, if you click **Exit**, you must enter these details in Microsoft Outlook. Server details include:

- **Secure Meeting Settings**—PBMA’s implementation of this tool requires this setting to remain blank.
- **Secure Meeting Hostname**—PBMA SecureMeeting’s Hostname is `securemeeting.grc.nasa.gov`.
- **User Id**—Your SecureMeeting username – *lastname.firstname*.
- **Password**—Your SecureMeeting password.
- **Realm**—leave default – *Users*.

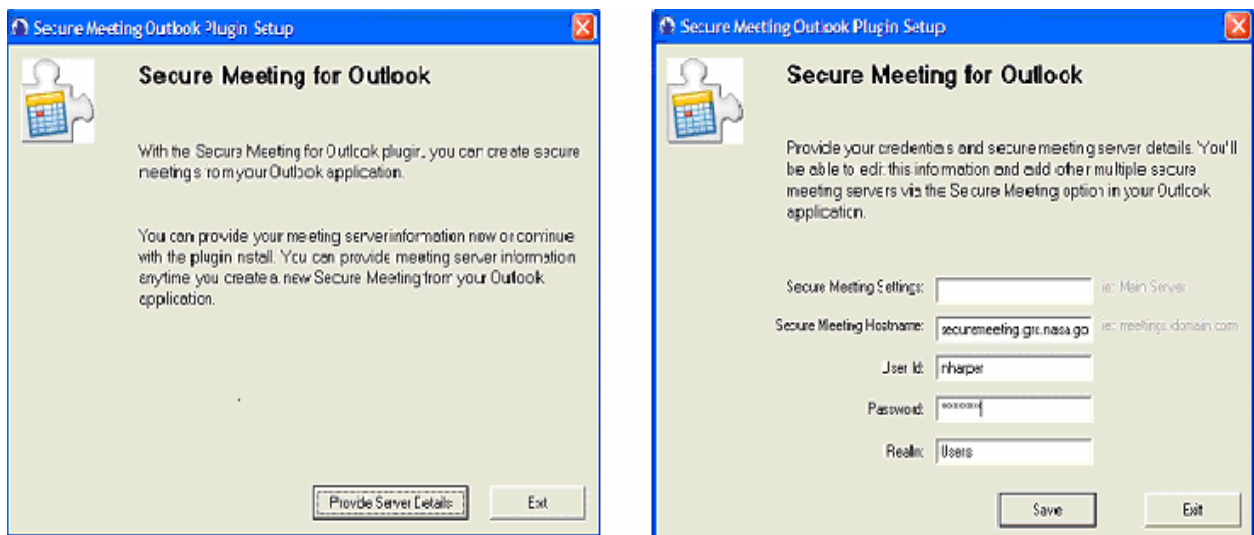


Figure 11 - MS Outlook Plug-in Setup

- Click **Save**.
- Click **Exit**.
- Reopen Outlook to begin scheduling meetings.

4.1.3.2 Scheduling Meetings Through Microsoft Outlook

- Open Microsoft Outlook.
- From the **File** menu, choose **New > Secure Meeting** or click the Secure Meeting tab as seen in Figure 12.

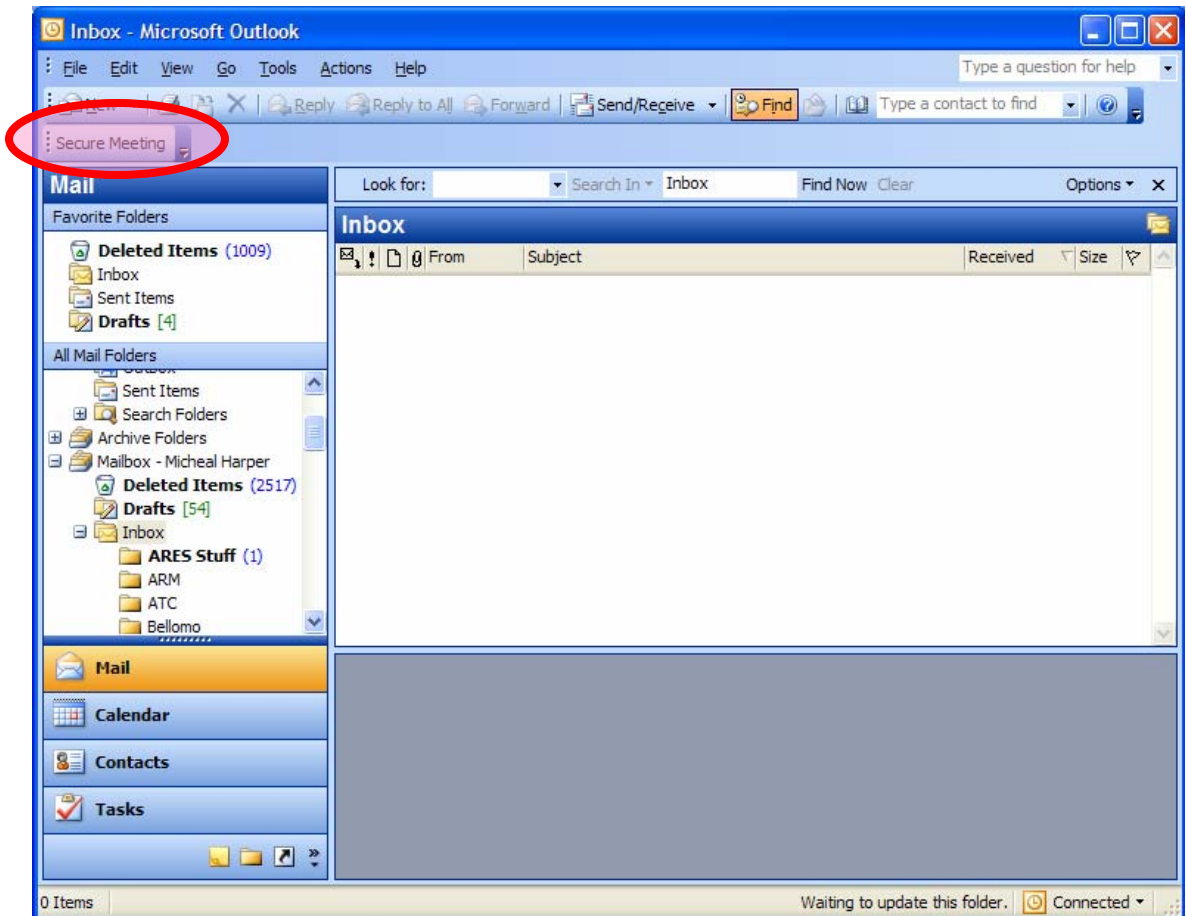


Figure 12 - Microsoft Outlook

- In the **Secure Meeting** tab, specify a password for the meeting as well as a telephone number that invitees should call to teleconference into the meeting (both optional).
- From the **Secure Meeting Servers** tab, ensure that the following information is entered:
 - **Secure Meeting Settings**—leave default - securemeeting.grc.nasa.gov
 - **Secure Meeting Settings**—PBMA's implementation of this tool requires this setting to remain blank.
 - **Secure Meeting Hostname**—PBMA SecureMeeting's Hostname is securemeeting.grc.nasa.gov.
 - **User Id**—Your SecureMeeting username – *lastname.firstname*.
 - **Password**—Your SecureMeeting password.
 - **Do not save password locally**—Select this checkbox to prevent the Secure Meeting for Outlook plug-in from storing an encrypted version of your password on your local system.
 - **Realm**—leave default – *Users*.

- Use the Outlook's standard functionality in the **Appointment** and **Scheduling** tabs to specify meeting details. Note that Secure Meeting supports creating standard or recurring meetings through Outlook.

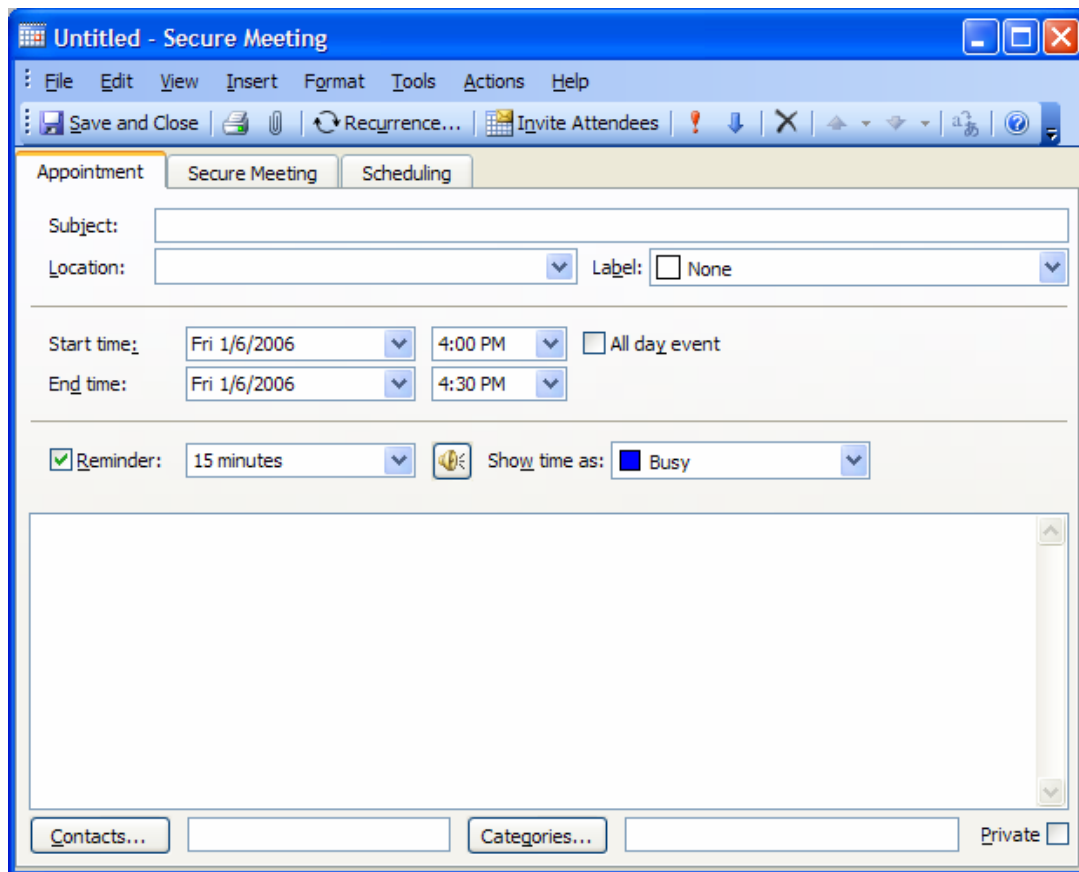


Figure 13 - Outlook Appointment and Scheduling Interface

- Use Outlook's **Save and Close** or **Send** button to finish processing your meeting. Outlook stores the details that you specified in the **Secure Meeting** tab and makes them available to you the next time you schedule a meeting from Outlook.
- Also, when you choose **Send**, Outlook sends invitation emails to the invitees using the text and meeting URL link constructed by the Secure Meeting for Outlook plug-in. Outlook adds the meeting to the Outlook calendars of meeting invitees. This calendar item includes all of the standard information recorded by Outlook as well as an additional **Secure Meeting** tab containing the information specified by the meeting creator.

4.2 Attending Meetings

4.2.1 PBMA SecureMeeting Supported Environments

SecureMeeting is designed to work in a variety of environments. Depending on how your system is configured however, SecureMeeting may operate differently and provide different levels of functionality, as described in the following sections.

The easiest way to determine if your system is compatible with the SecureMeeting application, however, is to use the SecureMeeting Compatibility Checker. To use this feature, go to the meeting sign-in page using the meeting URL:

<https://securemeeting.grc.nasa.gov/meeting/>

Once on this web page, click the link *Check Meeting Compatibility* as shown in Figure 14.

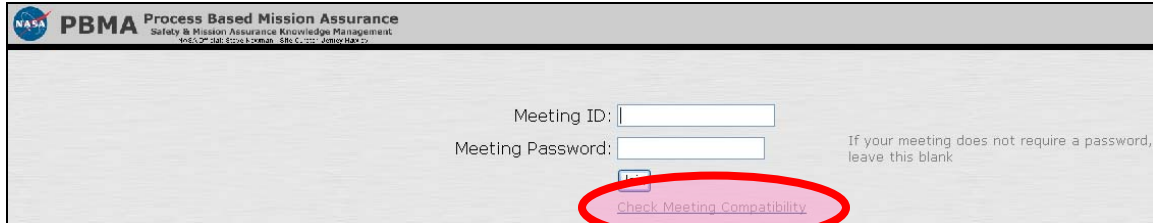


Figure 14 - The Check Meeting Compatibility Link

This tool determines your compatibility level and suggests upgrades to achieve full compatibility if required. You may run the Compatibility checker at any time after scheduling a meeting - you do not have to wait until the meeting is about to begin.

Note: The SecureMeeting compatibility checker does not check your connection speed or other miscellaneous factors that will not affect your system's compatibility, but may affect your meeting experience.

4.2.1.1 Operating system and browser requirements

PBMA SecureMeeting is supported at different levels on different operating systems. If you run SecureMeeting on a:

- **Windows operating system** - You can access all meeting functionality. Supported Windows operating systems include Windows 98 SE, Windows ME, Windows 2000 with service pack 4, Windows NT 4.0 with service pack 6, and Windows XP with service pack 1. Supported browsers on Windows operating systems include Internet Explorer 6.0 with service pack 1 and Netscape Navigator 7.1. Additionally, Internet Explorer versions 5.0 and 5.5 with service pack 2 are supported on all of the Windows operating systems listed above except Windows XP.

- **Non-Windows operating system** - You can view, conduct, or remote control a meeting, but cannot present. Secure Meeting should work on any operating system with the correct Java Virtual Machine (JVM) installed on it, but we recommend MacX 10.3 with Safari 1.1.1 or Linux Redhat 7.3 with Mozilla 1.1 in non-Windows environments. In addition to the browser requirements listed above, you must also enable javascript and one of the following components through your browser. If Active-X components are enabled through your browser, SecureMeeting downloads an Active-X component onto your client machine when you join a meeting. Otherwise, if you have a JVM installed, SecureMeeting downloads a Java applet when you join a meeting:
 - **Active X components**—Active-X controls are automatically enabled for administrators and power users on Windows 2000 systems, but standard users must enable them manually. To enable Active-X controls in Internet Explorer*, choose **Tools > Internet Options > Security > Custom Level**, and then enable Active-X components through the **Security Settings** dialog box.
 - **Microsoft Java Virtual Machine (JVM)**—To enable Microsoft JVM in Internet Explorer*, choose **Tools > Internet Options > Security > Custom Level**, and then enable **Microsoft VM** through the **Security Settings** dialog box.
 - **Sun Java Virtual Machine (JVM) 1.4 .1_01 or above**—Secure Meeting runs a Java applet in memory on your machine when you join a meeting. Secure Meeting is supported with Sun JVMs versions 1.4.1_01 and above. You can download the Sun JVM from www.java.com.

To enable Javascript through:

- **Internet Explorer***—Navigate to **Tools > Internet Options > Security** tab, and choose **Custom Level**. Under **Scripting of Java applets**, choose **Enable**.
- **Netscape Navigator***—Navigate to **Edit > Preferences**. Under **Advanced > Scripts & Plugins**, select the **Navigator** check box.

4.2.1.2 Additional requirements and restrictions

PBMA SecureMeeting supports running meetings with monitor displays up to 32-bit color. PBMA SecureMeeting cannot be used to share streaming media applications.

4.2.2 Accessing the Meeting URL

To attend a meeting, PBMA SecureMeeting invitees must navigate to the meeting site using their SecureMeeting Account. The following steps outline the way in which a SecureMeeting invitee receives notification of a meeting.

* The instructions shown here are for the latest browser versions. Instructions may vary for older browsers.

1. The invitee will receive an email that will contain the meeting time, duration, date, agenda, teleconference information, meeting venue URL, and system compatibility checker URL. An example of this email is shown below in Figure 15.
2. Click the URL under the *Meeting Venue* provided in the SecureMeeting notification email and you will receive the **SecureMeeting** login web page.

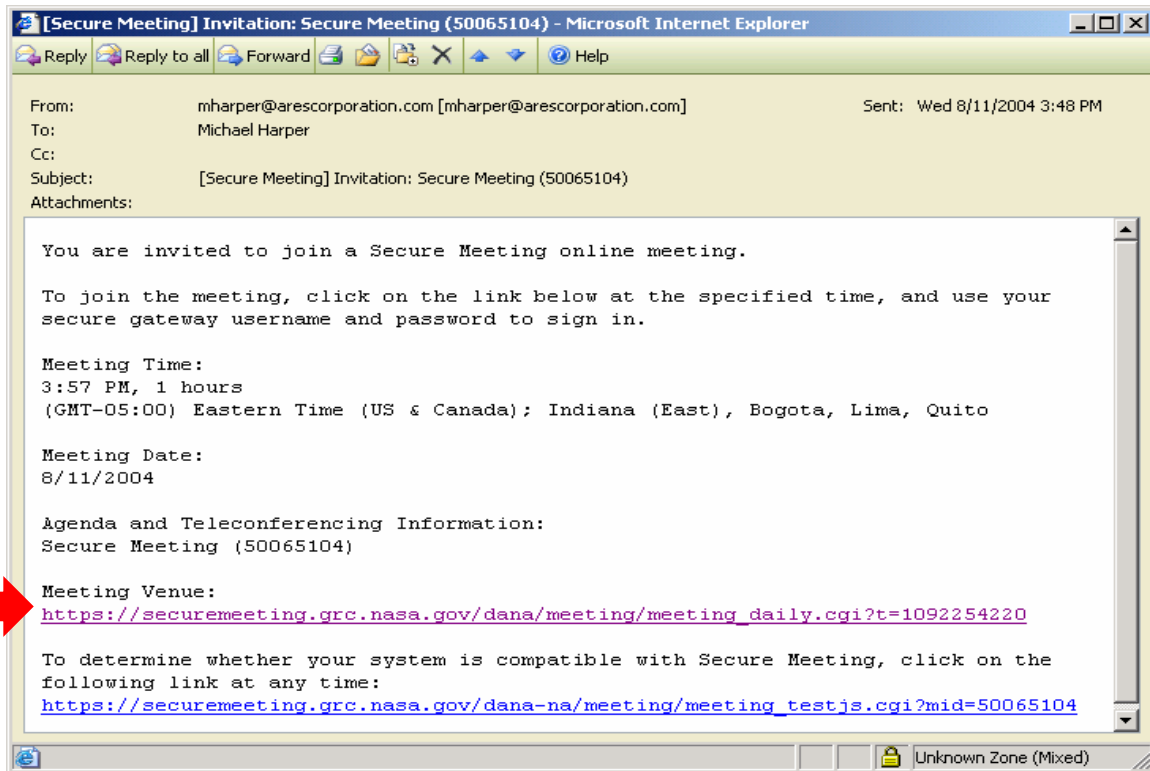


Figure 15 - Sample Invitation Email

3. Click the *Meeting* link provided on the **SecureMeeting Welcome** Web Page as shown in Figure 5.
4. The link will take you to the **SecureMeeting Calendar** Web page as in Figure 16, where you can view all meetings that you have scheduled or been invited to participate in.
5. The meeting that you are to join will show up in your calendar. Click the *Join Meeting* link, circled in red below.

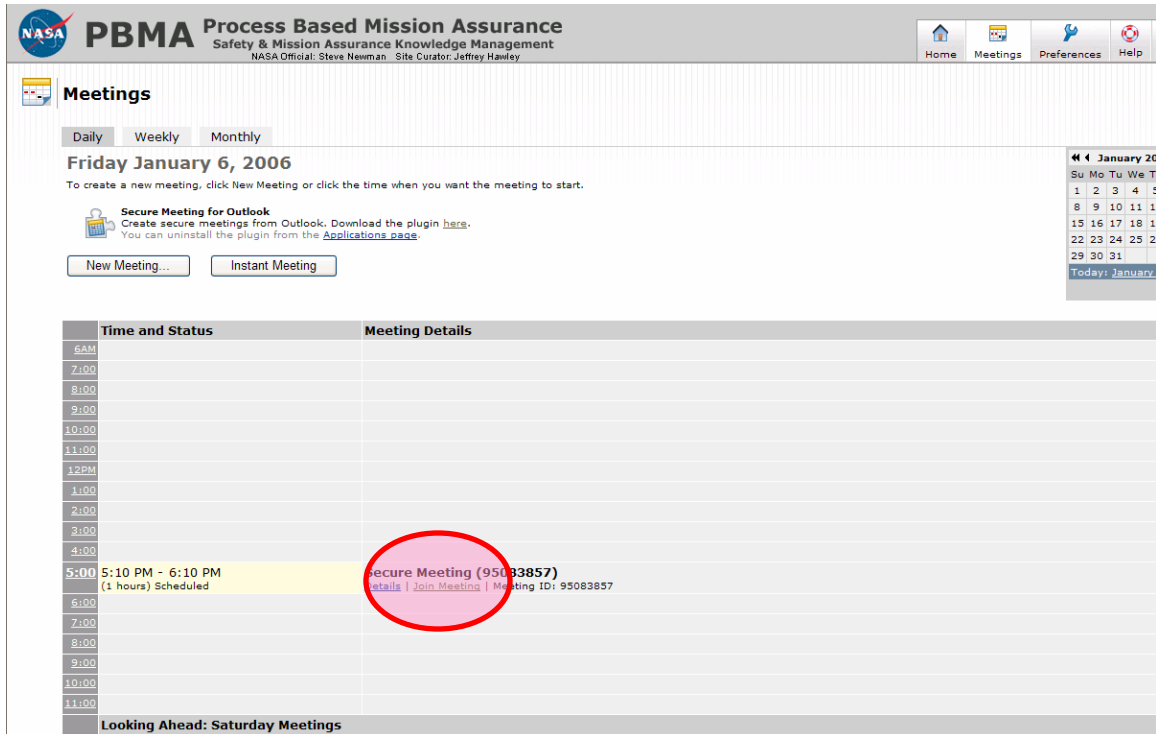


Figure 16 - SecureMeeting Calendar

6. The **Join Meeting** Web page will appear. Click the *Join Meeting* button to enter the meeting.

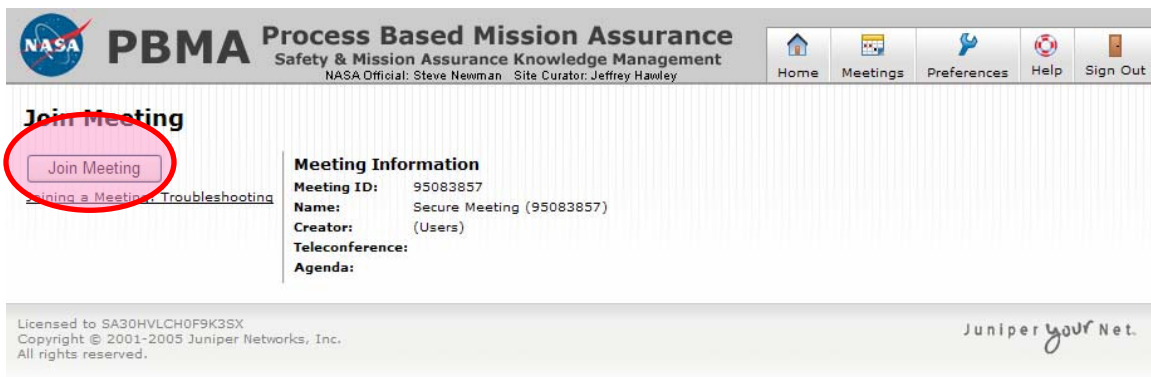


Figure 17 - The Join Meeting Button

4.2.3 Joining the Meeting

When the invitee chooses to join a meeting, the PBMA SecureMeeting application downloads either an Active-X component or a Java applet onto the invitee's system. Again, if Active-X components are enabled through your browser, SecureMeeting downloads an Active-X component onto your client machine when you join a meeting. Otherwise, if you have a JVM installed, SecureMeeting downloads a Java applet when you join a meeting. This client-side component contains:

- a meeting viewer
- presentation tools
- a text messaging application

Once PBMA SecureMeeting launches the Active-X or Java applet on the user's desktop, the user becomes a meeting attendee and can begin participating in the meeting. Attendees are allowed to join up to 15 minutes before the meeting is scheduled to start.

4.2.4 Meeting Viewer

Once the meeting scheduler or invitee clicks the *Start Meeting* or *Join Meeting* button, the **Meeting Viewer** window will be launched. The window appears as in Figure 18.

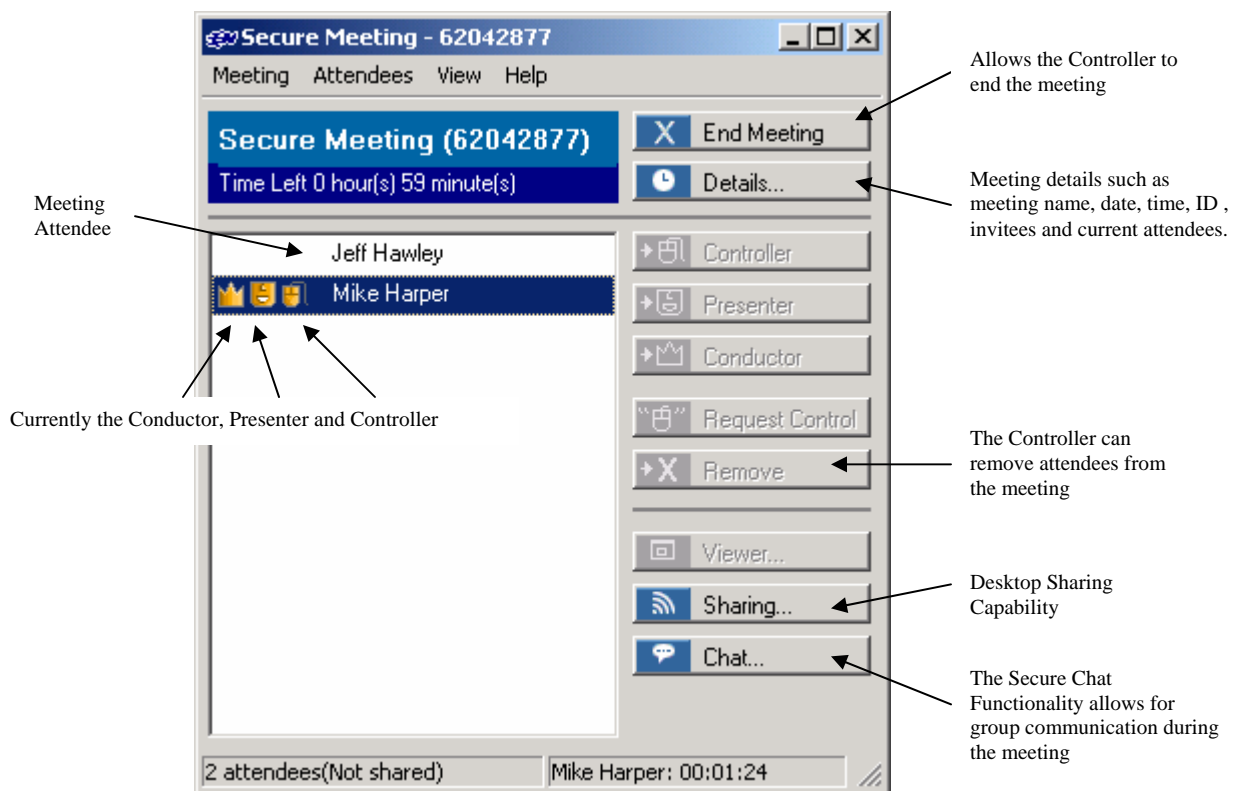


Figure 18 - The Meeting Viewer Window

4.2.4 Viewing a Meeting

If you are a meeting viewer, you simply need to join the meeting to begin viewing the presentation. Secure Meeting automatically opens the Secure Meeting Viewer window on your desktop when the presenter begins sharing. Then, if you want to:

- Switch the presentation to full-screen mode, select the *View* pull-down menu and click on *Full Screen*.
- Switch back and forth between full-screen and reduced-screen mode, press *Ctrl + F*.

- Close the **Meeting Viewer** window, select the *View* pull-down menu and click on *Close*.


If you open other windows or applications (such as the Secure Meeting Chat window) in front of the view window during a presentation, you can return to the Secure Meeting Viewer window simply by clicking its icon on the Secure Meeting task bar or the Windows task bar at the bottom of your screen.


Note: If you see a gray screen in the Secure Meeting Viewer window, you may need to alert the meeting presenter. To protect the presenter's privacy, SecureMeeting only displays those applications that the presenter has chosen to share in the view windows of the meeting attendees. If the presenter is working with an unshared application, meeting attendees simply see gray.


4.3 Running Meetings

4.3.1 Meeting Roles and Functionality

Within the Secure Meeting window, Secure Meeting displays an icon next to the attendees who have meeting responsibilities beyond viewing. These icons indicate the attendee's meeting role and corresponding responsibilities:

 **Conductor**—The conductor is responsible for starting a meeting, extending the meeting if it runs over the scheduled duration, expelling meeting attendees if necessary, and closing the meeting when it is done. By default, the conductor is also the presenter and controller. For more information, see *Conducting Meetings*.

 **Presenter**—The presenter is responsible for presenting his desktop or applications to other meeting attendees and also controls who may annotate his presentation. For more information, see *Presenting Applications*.

 **Controller**—The controller is responsible for using his mouse and keyboard to operate the shared applications running on the presenter's computer. The presenter is always one of the meeting's controllers, but may choose to allow another user to jointly control the shared applications. For more information, see *Controlling Applications*.

The individual who scheduled the meeting is the default **Meeting Conductor** ("Conductor") within the SecureMeeting application. Before the Conductor joins the meeting, the other attendees can only chat. They cannot view or make a presentation because the Conductor is also the default **Meeting Presenter** ("Presenter"). Finally, the individual starting the meeting is also the **Meeting Controller** ("Controller"). A Controller uses his or her own mouse and keyboard to remote control the Presenter's shared desktop or applications.

The Conductor is responsible for starting the meeting, ending the meeting and assigning the Presenter role if he or she chooses.

4.3.2 Passing Presenter Rights to Another Attendee

The Conductor may designate any other SecureMeeting account owner as a Conductor and any other Windows user attendee as a Presenter. For example, you may need to ask another attendee to present an application that is not installed on your computer. The attendee that you designate may then display their desktop or applications to other attendees.

Note: Only the meeting conductor can change who presents during a meeting.

To hand over presentation control to someone else in a meeting:

1. Select the attendee to whom you want to pass presenter rights by clicking on his or her login name in the **Secure Meeting** window.
2. Click the *Presenter* button. Alternatively, select the *Attendees* pull-down menu and click on the *Set as Presenter* button. The selected attendee may now present.
3. To take back presenter rights, click on your own name in the **Secure Meeting** window and click the *Presenter* button.

4.3.3 Passing Conductor Rights to Another Attendee

If you are the meeting conductor, you may pass conductor rights to any other in-network attendee (that is, any other user who is signed into the same Secure Meeting server as the meeting creator). For instance, you may need to leave early and ask another user to oversee the remainder of the meeting.

To pass conductor rights to another in-network attendee:

1. Select the meeting attendee to whom you want to pass conductor rights by clicking on their login name in the **Secure Meeting** window.
2. Click the *Conductor* button. Alternatively, select the *Attendees* pull-down menu and click *Set as Conductor*. The selected attendee may now conduct the meeting.

Note: If you want to regain conductor rights, the new conductor must grant them to you.

4.3.4 Passing Controller Rights to Another Attendee

If you are a meeting viewer, you may request control of the presenter's desktop or shared application(s). If the presenter then chooses to grant your request (as described in Sharing Controller Rights with Another Attendee), the two of you jointly share control—both of you can use your mice and keyboards to operate the presenter's shared resources.

To request control:

1. Select the presenter's name by clicking on their login name in the **Secure Meeting** window.
2. Click the *Request Control* button. Alternatively, select the *Attendees* pull-down menu and click on *Request Control*.
3. If the presenter allows you access, find the resource that you want to control in the **Secure Meeting Viewer** window, click your mouse in the application, and begin typing or otherwise operating the application.

When you are remote controlling, you and the presenter are jointly controlling the application (trading off, if necessary) although only one of you may actively control the application at any given time.

You can determine who is actively controlling the application through the Secure Meeting window—a yellow controller icon appears next to the active controller's name, whereas a gray controller icon appears next to the passive controller's name. If you are passively controlling the application and want to actively control it, simply click again in the application.

When the Presenter wants to regain control of his remote-controlled applications, he or she simply needs to right-click anywhere on the screen and SecureMeeting returns control.

4.3.5 Desktop Sharing

The Conductor (or a meeting attendee that is designated as a Presenter) starts the meeting presentation by sharing his desktop or applications with other attendees. Once the Presenter begins sharing, a meeting viewer automatically opens on all of the meeting attendees' desktops and displays the presenter's shared application*.

To present your desktop or application(s) to other meeting attendees:

1. Open the applications you want to present to other attendees.
2. Click the *Sharing* button in the **Secure Meeting** window. The **Share Applications** window, as shown in Figure 19, will appear.

* Secure Meeting cannot display the content of a meeting presenter's desktop if it is locked.

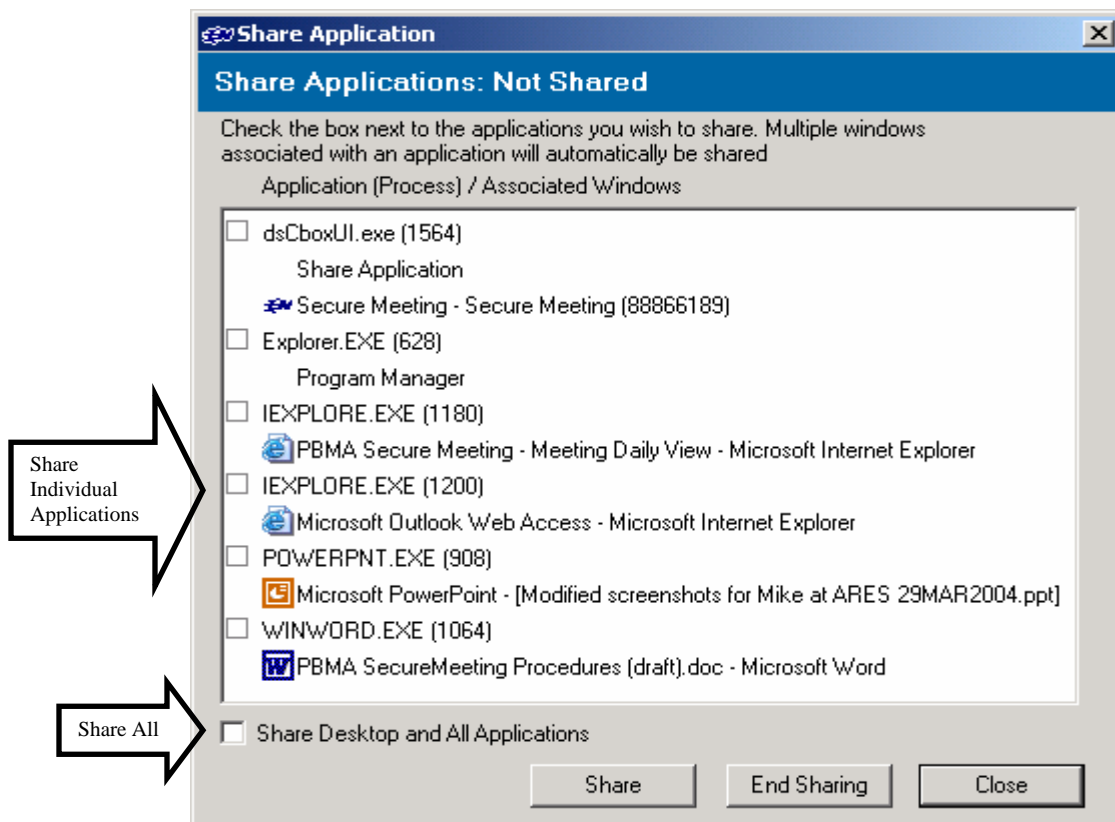


Figure 19 - The Share Application Window

3. Determine what you want to share with the meeting attendees. You have the option to share:
 - a. Your entire desktop (including all of the applications you currently have open). To do so, select the *Share Desktop and All Applications* checkbox at the bottom of the dialog box.
 - b. An isolated application (or applications). To do so, select the checkboxes next to those applications that you want to share in the Application (Process)/Associated Windows list and then click the *Share* button.
4. To stop presenting your desktop or applications to other meeting attendees, choose *End Sharing* in the Share Applications dialog box.

Note the following:

- When you select an application window in the Share Application page, Secure Meeting automatically selects all application windows that share a process with the selected window. For example, if you select an Internet browser window that you originally opened from within another browser window, Secure Meeting automatically selects both windows.

- Macintosh users can share their entire desktop, but not individual applications.
- A gray screen appears on the screens of the meeting attendees when you move an unshared application in front of a shared application(s) on your desktop. Secure Meeting uses the gray screen to protect your privacy and cover any information that you do not want to share.
- If you share an application or your desktop and then lock your workstation, Secure Meeting stops presenting your application(s) to meeting viewers. We recommend that you pass presentation rights to another meeting attendee before locking your workstation.
- If you share your desktop and then let your system remain idle, Secure Meeting displays any screen savers or screen sleep activity that appears on your system to meeting attendees, making it appear as if the presentation has stopped.

4.3.6 Secure Chat Functionality

The Secure Chat Functionality allows for group communication during the meeting and all attendees can access the chat feature. As soon as an attendee joins a meeting, they may start sending text messages to one other using the “SecureMeeting Chat” window, even if the Controller has not yet joined.

By default, the chat window is closed during the meeting. You must manually open it to start chatting. Once any one meeting attendee sends a text message, however, Secure Meeting automatically:

- Opens the chat window on all of the other attendees’ desktops so that they can see the message and respond.
- Alerts the other attendees that the chat window is open by flashing a chat window item in the attendees’ task bars at the bottom of their screens.

To send text messages using the chat window:

1. Open the chat window console using one of the following methods:
 - i. From the **Secure Meeting** window’s *View* menu, select *Chat*.
 - ii. In the **Secure Meeting** window’s task bar, click the *Chat* button.
 - iii. Click the meeting console’s icon in your task bar.
2. The **Secure Meeting Chat** window as shown in Figure 20 will appear. Type your text in the bottom of the chat window and press *Enter* or click the *Send* button.

3. To exit the discussion, from the **Secure Meeting Chat** window's *File* pull-down menu, select Close.

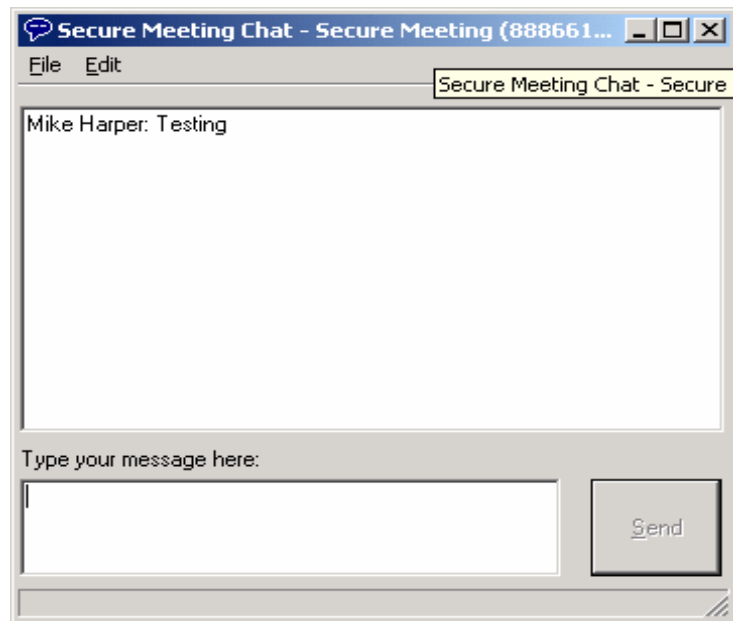





Figure 20 - The Secure Meeting Chat Window


4.3.7 Desktop Drawing

If you are the meeting presenter, you may annotate the presentation on screen to call attention to a specific part of the display. If the desktop or at least one of the applications are being shared, then the Draw button and related drawing buttons to its right in the toolbar at the top of the screen will no longer be grayed out. Click the *Draw* button to start drawing. Depending on what you want to annotate on screen, use any of the following buttons:

 **Draw**—If you are not the meeting presenter but you want to annotate the presentation, use the drop-down option to request drawing permissions. When you do, a request appears on the presenter's desktop and she may decide whether or not you can annotate the presentation. If you are the meeting presenter, use the drop-down options to control who may annotate the presentation.

 **Show/Hide Drawing**—Click this icon to show or hide drawings. Note that if you choose to hide drawings, Secure Meeting does not display any new drawings that are created until you click the icon back into the “show” position.

 **Select Cursor Type**—Use the drop-down options to change your cursor type to a standard arrow, large red arrow, or target.

 **Select Drawing Shape**—Use the drop-down options to select an annotation shape. Possible types include lines, blocks, and circles.

T Type Text—Click this icon to add text to the presentation. When you do, Secure Meeting creates a yellow box to contain any text that you type.

🗑 Delete Drawing—Use the drop-down options to delete some or all of the annotations that have been added to the presentation.

■ Select Color—Use the drop-down options to select a color for the lines, circles, and blocks that you add to the presentation.

■ Select Size—Use the drop-down options to select a size for the lines, circles, and blocks that you add to the presentation.

An example of multiple annotations on a given document can be seen in Figure 21.

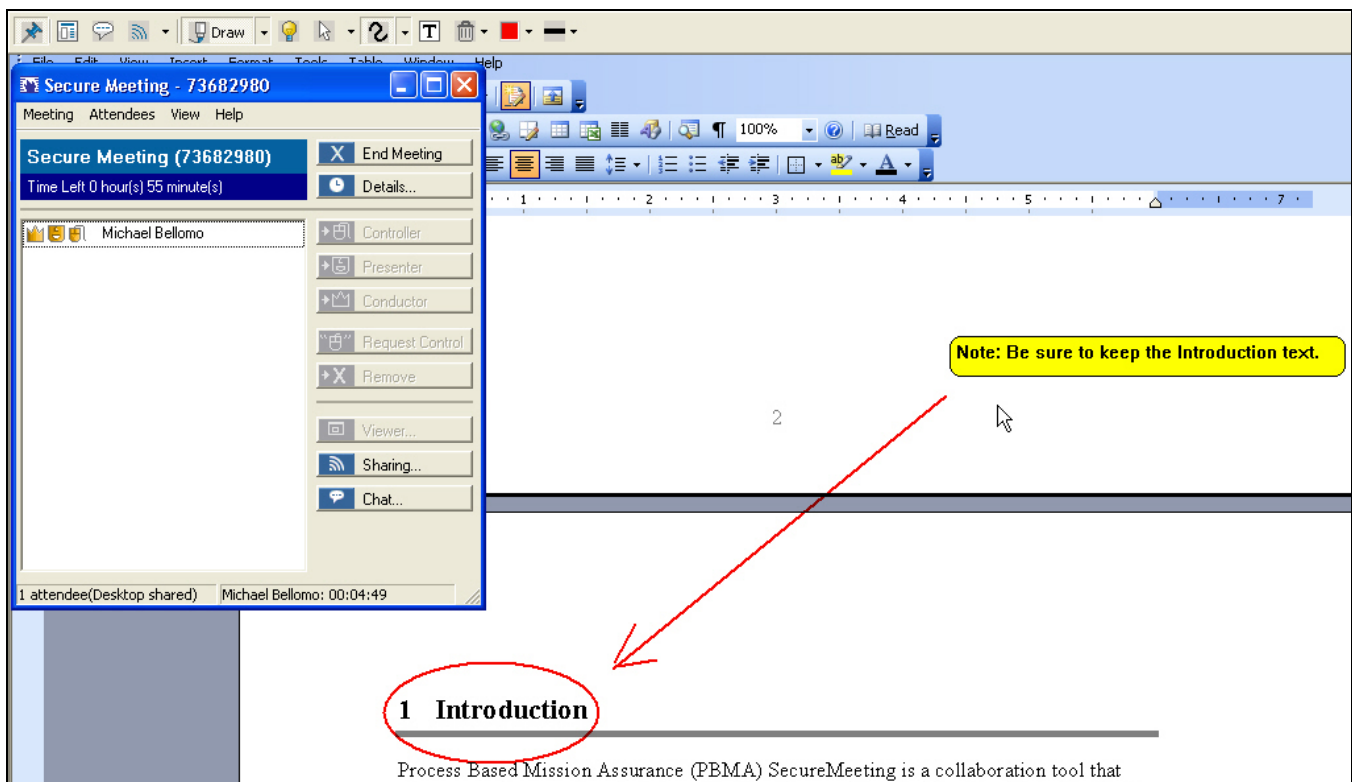


Figure 21 - A Drawing Sample showing Circles, Straight Lines, and Text

4.3.8 Removing Attendees

If you are the meeting conductor, you may find it necessary during the course of the meeting to remove an attendee. For instance, the presenter may experience problems with the application that he is sharing. If you decide that the presenter's difficulties are slowing down the meeting, or that the attendees should not see the problems, you can simply remove the presenter from the meeting. Once the problems are fixed, the former presenter can rejoin the meeting in progress.

To remove an attendee from a meeting:

1. Select the attendee that you want to expel by clicking on his or her user name in the **Secure Meeting** window.
2. Click the Remove button. Alternatively, from the *Attendees* pull-down menu, select *Remove Attendee*.
3. When prompted, confirm that you want to remove the attendee by clicking the *Confirm* button.

Note: Attendees may return to a meeting after being removed.

4.3.9 Extending Meetings

If you are the meeting conductor, you may decide during the course of a meeting that the original duration specified by the meeting's creator is not adequate.

To extend the duration of a meeting:

1. Click the *Details* button in the **Secure Meeting** window.
2. The **Meeting Details** window will appear. Specify how much longer you want the meeting to run in the *Extend Meeting By* field.
3. Click the *Extend* button.
4. Click the *Close* button.

4.3.10 Closing Meetings

A meeting ends when it has run for the scheduled amount of time or the maximum duration allowed by the Secure Meeting administrator. If you are the meeting conductor or creator, Secure Meeting provides you with several additional mechanisms for ending a meeting. The meeting conductor may end a meeting using any of the following methods:

- From the Secure Meeting window's *Meeting* pull-down menu, select *End Meeting*.
- Click the *End Meeting* button in the Secure Meeting window.
- Leave the meeting—Secure Meeting ends the meeting 1 hour after you leave.
- Leave your secure gateway session.

5 Getting Help

PBMA Technical Support is available if you encounter any problems with the PBMA SecureMeeting system. Help can also be accessed at anytime while logged into the SecureMeeting system. The *Help* link is located on the right of the gray bar at the top of the page as seen in Figure 22.

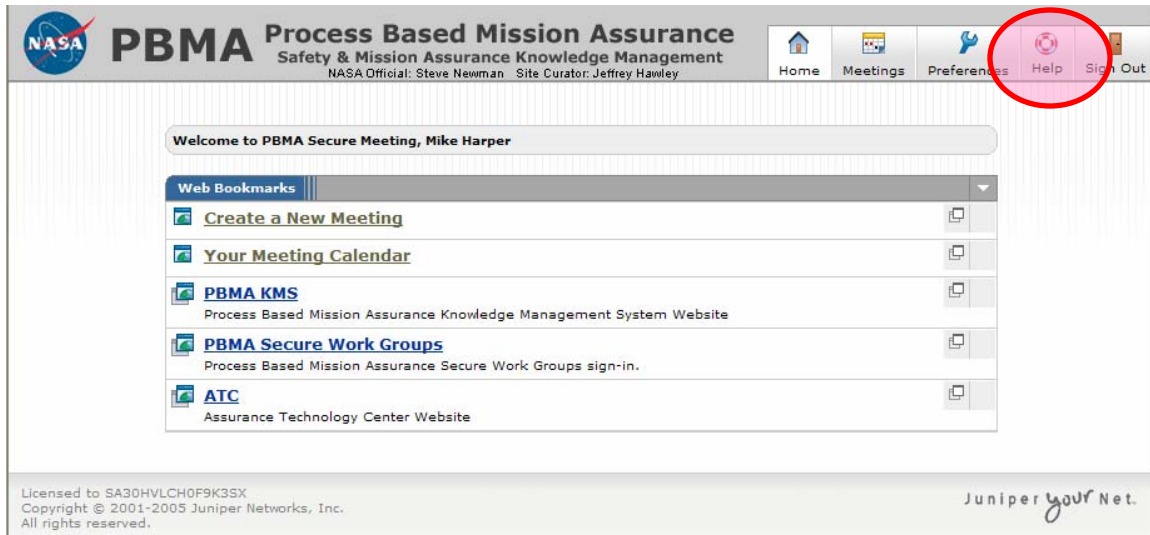


Figure 22 - The Help Link

The **Help Window** is generated as in Figure 23. You can look up the area where you need help in the applications table of contents, listed on the left hand side of the window.

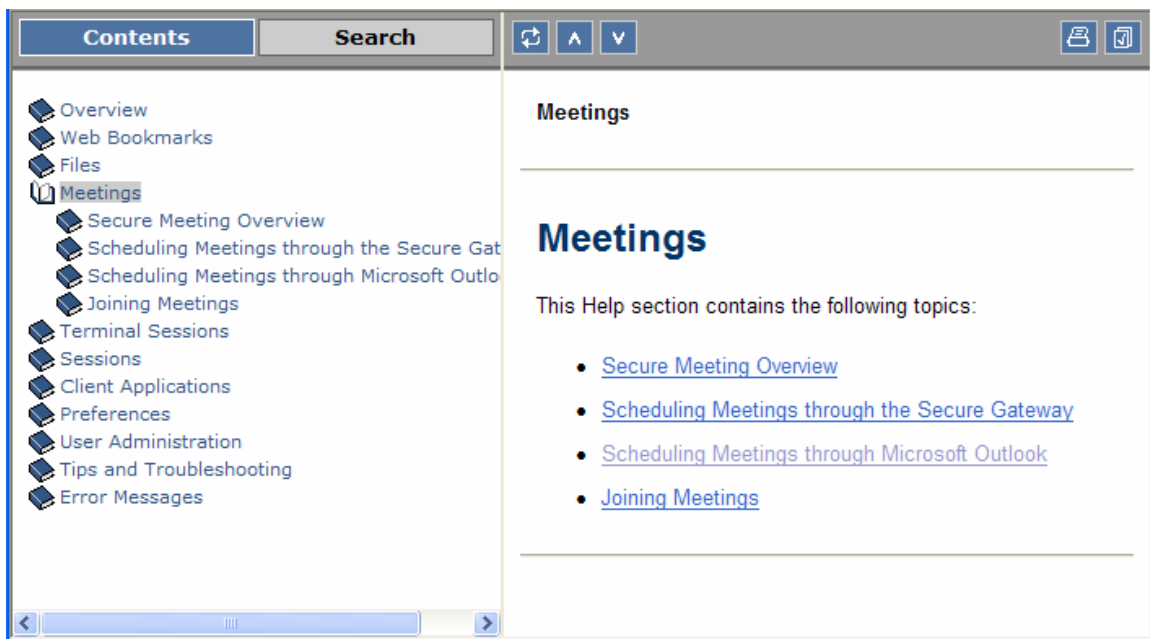


Figure 23 - The Help Window

Technical support is also available when the information provided in this document and online **Help Window** proves insufficient. Technical Support can be contacted via email at pbma.admin@arescorporation.com.

All issues sent to Technical Support pertaining to the SecureMeeting application should have “PBMA SecureMeeting” in the subject line. Additionally, the following information must be in the email to PBMA Technical Support:

- Name
- Work Phone
- Description of the Problem or Request

In addition to the information identified above, please have the following available if Technical Support should need to contact you by telephone:

- Steps to re-create problem, if known
- System information
 - Browser - Application (Internet Explorer or Netscape) and version
 - Operating System - Application (Windows or Mac) and version
- Access location
 - Center/facility or organization

Standard operating hours of Technical Support are Monday through Friday 8:00 AM to 5:00 PM EST. Technical Support will observe all NASA holidays. Any requests received outside of standard operating hours will be handled as soon as possible the following business day.